Math 418/818
Assignment 6 - Solutions

[3] 1. (a) By Property (P1) we know that if $x \in G$, then $x \in G[m] \iff \text{ord}(x) \mid m$, and so $G[m] = \{x \in G : \text{ord}(x) \mid m\} = \bigcup_{d|m} G(d)$, where $G(d) := \{x \in G : \text{ord}(x) = d\}$. By Q1 of Assignment #5 we know that $|G(d)| = \phi(d)$, if $d \mid n$ (which is the case if $d \mid m$). Thus $|G[m]| = \sum_{d|m} \phi(d)$ because the sets $G(d)$ are pairwise distinct.

It remains to show that $\sum_{d|m} \phi(d) = m$. For this, let $S = \{1, 2, \ldots, m\}$, and for a divisor $d \mid m$ put $S_d = \{x \in S : \text{gcd}(x, n) = d\}$. Thus $S = \bigcup_{d|m} S_d$, so $m = |S| = \sum_{d|m} |S_d|$ because the sets $S_d$ are distinct. Now $x \in S_d \iff x = x'd$, where $1 \leq x' < \frac{n}{d}$ and $\text{gcd}(x', \frac{n}{d}) = 1$, so $S_d = \{x'd : 1 \leq x' < \frac{n}{d}, \text{gcd}(x', \frac{n}{d}) = 1\}$, and hence $|S_d| = \phi\left(\frac{n}{d}\right)$. Thus $m = \sum_{d|m} \phi\left(\frac{n}{d}\right) = \sum_{d \mid m} \phi(d)$, the latter because if $d$ runs over all divisors, then so does $d' = \frac{n}{d}$. Thus $|G[m]| = \sum_{d|m} \phi(d) = m$, as desired.

(b) For any $k \in \mathbb{Z}$ we have that $(\langle x \rangle^k)^m = x^{nk} = 1$, so $\langle x \rangle^k \in G[m]$ and thus $\langle x \rangle^k \subseteq G[m]$. Since $\text{ord}(x^k) = m$ by Property (P2), we have by Theorem 2.1 in class that $|\langle x \rangle^k| = \text{ord}(x^k) = m = |G[m]|$ by part (a), and so $G[m] = \langle x \rangle^k$.

(c) Let $x = (x_1, x_2) \in G = G_1 \times G_2$. Then $x^m = (x_1^m, x_2^m)$, so $x \in G[m] \iff (x_1^m, x_2^m) = (1, 1) \iff x_1 \in G_1[m]$ and $x_2 \in G_2[m] \iff x = (x_1, x_2) \in G_1[m] \times G_2[m]$, so $G[m] = G_1[m] \times G_2[m]$.

Since $65 = 5 \cdot 13$, we have by CRT that $G := (\mathbb{Z}/65\mathbb{Z})^\times \cong G_1 \times G_2$, where $G_1 = (\mathbb{Z}/5\mathbb{Z})^\times$ and $G_2 = (\mathbb{Z}/13\mathbb{Z})^\times$. Since 5 and 13 are primes, we know that $G_1$ is cyclic of order 4 and $G_2$ is cyclic of order 12, so by part (a) we see that $|G_1[4]| = 4$ for $i = 1, 2$, and hence $|G[4]| = |G_1[4] \times G_2[4]| = 4 \cdot 4 = 16$.

[4] 2. (a) Since $n = |\mathbb{F}_{181}^\times| = 180 = 2^2 \cdot 3^2 \cdot 5$ and $b = 2$ in both cases, we first precompute the power/log tables for $c_p = 2^{n/p}$ for $p = 2, 3$ and 5. Using Maple, we see that $c_2 = 2^{180/2} \equiv 180 \pmod{181}$, $c_3 = 2^{60/3} \equiv 48 \pmod{181}$, $c_5 = 2^{36/5} \equiv 59 \pmod{181}$. Since $48^2 \equiv 132 \pmod{181}$ and $59^2 \equiv 42 \pmod{181}$, $59^4 \equiv 135 \pmod{181}$, the respective log tables are as follows:

<table>
<thead>
<tr>
<th>$y = c_2^x$</th>
<th>1</th>
<th>180</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_{c_2}(y)$</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$y = c_3^x$</th>
<th>1</th>
<th>48</th>
<th>132</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_{c_3}(y)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$y = c_5^x$</th>
<th>1</th>
<th>59</th>
<th>42</th>
<th>125</th>
<th>135</th>
</tr>
</thead>
<tbody>
<tr>
<td>$D_{c_5}(y)$</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>

(i) Calculating $x = DL_2(y)$, for $y = 103$:

For $p = 2$ we obtain

$y_0 = y \equiv 103 \pmod{181}$ and $y_0^{n/p} = 103^{180/2} \equiv 180 \pmod{181}$ \Rightarrow $x_0 = DL_{c_2}(180) = 1$

$y_1 = y_0 / b^{x_0} \equiv 142 \pmod{181}$ and $y_1^{n/p^2} = 142^{180/4} \equiv 180 \pmod{181}$ \Rightarrow $x_1 = DL_{c_2}(180) = 1$

Thus $x \equiv x_0 + x_1 p \equiv 1 + 1 \cdot 2 \equiv 3 \pmod{4}$. Similarly, for $p = 3$:

$y_0 = y \equiv 103 \pmod{181}$ and $y_0^{n/p} = 103^{180/3} \equiv 132 \pmod{181}$ \Rightarrow $x_0 = DL_{c_3}(132) = 2$

$y_1 = y_0 / b^{x_0} \equiv 71 \pmod{181}$ and $y_1^{n/p^2} = 71^{180/9} \equiv 48 \pmod{181}$ \Rightarrow $x_1 = DL_{c_2}(48) = 1$

Thus $x \equiv x_0 + x_1 p \equiv 2 + 1 \cdot 3 \equiv 5 \pmod{9}$. Finally, for $p = 5$ we have $y_0 = y^{n/p} = 103^{180/5} \equiv 59 \pmod{181}$, so $x_0 = DL_{c_5}(y_0) = DL_{c_5}(59) = 1$. Thus $x \equiv x_0 \equiv 1 \pmod{5}$, and hence we have the congruences

$x \equiv 3 \pmod{4}, \quad x \equiv 5 \pmod{9}, \quad x \equiv 1 \pmod{5}$.

We apply CRT with $m_1 = 4$, $m_2 = 9$ and $m_3 = 5$. Here $m_1^* = 1 \pmod{4}$, $m_2^* = 5 \pmod{9}$, and $m_3^* = 1 \pmod{5}$, so $e_1 = 45, e_2 = 100, e_3 = 36 \pmod{180}$. Thus $x \equiv 3e_1 + 5e_2 + 1e_3 \equiv 131 \pmod{180}$, which means that $DL_2(103) = 131$. Check: $2^{131} \equiv 103 \pmod{181}$.

(ii) Calculating $x = DL_2(y)$, for $y = 97$: 6–1
For $p = 2$ we obtain

\[
y_0 = y \equiv 97 \pmod{181} \quad \text{and} \quad y_0^{n/p} = 97^{180/2} \equiv 180 \pmod{181} \Rightarrow x_0 = DL_{c_2}(180) = 1
\]
\[
y_1 = y_0/b^{c_0} \equiv 139 \pmod{181} \quad \text{and} \quad y_1^{n/p^2} = 139^{180/4} \equiv 180 \pmod{181} \Rightarrow x_1 = DL_{c_2}(180) = 1
\]

Thus $x \equiv x_0 + x_1p \equiv 1 + 1 \cdot 2 \equiv 3 \pmod{4}$. Similarly, for $p = 3$:

\[
y_0 = y \equiv 97 \pmod{181} \quad \text{and} \quad y_0^{n/p} = 97^{180/3} \equiv 48 \pmod{181} \Rightarrow x_0 = DL_{c_3}(48) = 1
\]
\[
y_1 = y_0/b^{c_0} \equiv 139 \pmod{181} \quad \text{and} \quad y_1^{n/p^2} = 139^{180/9} \equiv 1 \pmod{181} \Rightarrow x_1 = DL_{c_3}(1) = 0
\]

Thus $x \equiv x_0 + x_1p \equiv 1 + 0 \cdot 3 \equiv 1 \pmod{9}$. Finally, for $p = 5$ we have $y^{n/p} = 97^{180/5} \equiv 125 \pmod{181}$ so $x_0 = DL_{c_5}(125) = 3$, and hence $x \equiv 3 \pmod{5}$. Thus:

\[
x \equiv 3 \pmod{4}, \quad x \equiv 1 \pmod{9} \quad x \equiv 3 \pmod{5}.
\]

We apply CRT with $m_1 = 4$, $m_2 = 9$ and $m_3 = 5$ again. As before, $e_1 \equiv 45, e_2 \equiv 100, e_3 \equiv 36 \pmod{180}$, and so $x \equiv 3e_1 + e_2 + 3e_3 \equiv 163 \pmod{180}$, i.e. $DL_2(97) = 163$.

[3] 3. By the result in class, the probability $P(p)$ is given by $\prod_{q | (p-1)} \left(1 - \frac{1}{q}\right)$.

(a) If $p = 101$, then $p - 1 = 100 = 2^25^2$, so $P(101) = (1 - \frac{1}{2})(1 - \frac{1}{5}) = \frac{2}{5} = 40\%$.

(b) If $p = 1019$, then $p - 1 = 1018 = 2 \cdot 509$, so $P(1019) = (1 - \frac{1}{2})(1 - \frac{1}{509}) = \frac{254}{509} \approx 49.9\%$

(c) If $p = 2311$, then $p - 1 = 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, so $P(2311) = (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})(1 - \frac{1}{7})(1 - \frac{1}{11}) = \frac{16}{117} \approx 20.78\%$.

[1] 4. (a) If $a \in (\mathbb{F}_p^\times)^2$, then by Q3 of Assignment #5 we know that ord$(a) | \frac{p-1}{2} < p - 1$, so $a$ cannot be a generator of $\mathbb{F}_p^\times$. This means that $a$ is not a primitive root mod $p$.

[2] (b) If $a$ is a primitive root mod $p$, then $a \notin (\mathbb{F}_p^\times)^2$ by part (a). Conversely, suppose that $a \notin (\mathbb{F}_p^\times)^2$. To show that $a$ is a generator (primitive root), it suffices to show that $a^{\frac{p-1}{r}} \neq 1$, for all primes $r | (p-1) = 2q$ (cf. Lemma in class). Now $a^2 \neq 1$ because $\mathbb{F}_p^\times[2] = \{1, -1\}$ (result in class), and $a \neq \pm 1$ by the hypothesis on $a$. Moreover, $a^q \neq 1$ because otherwise ord$(a) | q = \frac{p-1}{2}$ and then $a \in (\mathbb{F}_p^\times)^2$ by Q3 of Assignment #5. Thus, $a^{(p-1)/r} \neq 1$ for $r \in \{2, q\}$, and so $a$ is a generator.

[2*] (c) Since $q = 2n + 1$ is odd, we see that $p = 2(2n + 1) + 1 = 4n + 3 \equiv 3 \pmod{4}$. Thus, $-1 \notin (\mathbb{F}_p^\times)^2$ by Q3 of Assignment #5 and hence also $-4 \notin (\mathbb{F}_p^\times)^2$. Moreover, $-4 \neq -1 \pmod{p}$ (else $p | 3$, but 3 is not a safe prime). Thus, the hypotheses of part (b) hold, and so $-4$ is a generator.

[6] 5. (See the MAPLE solution on the course web-site.)